UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/895,508	06/29/2001	James S. Magdych	NAI1P011/01.116.01	7235

28875 7590 09/12/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 09/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/895,508
Filing Date: June 29, 2001
Appellant(s): MAGDYCH ET AL.

Kevin J. Zilka
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed July 7th, 2005.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

Appellant's brief includes a statement that claims

- 1, 12, 23-27;
- 1, 6, 9-10, 12, 17, 20-21, 23-30, 32;
- 4, 15;
- 5, 16;
- 34;
- 31;
- 35;
- 11, 22

do not stand or fall together and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

(8) Claims Appealed

Claims 1, 4-6, 9-12, 15-17, 20-32, and 34-35 are appealed.

Claim 33 is presented in the Appendix to the brief, but has not been appealed.

(9) Prior Art of Record

6,298,445	SHOSTACK et al.	10-2001
6,070,244	ORCHIER et al.	05-2000
4,386,233	SMID et al.	05-1983

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 12, 23-27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 4-6, 9-10, 12, 15-17, 20-21, 23-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (US Patent Number: 6,298,445, hereinafter "Shostack"), and further in view of Orchier et al. (US Patent Number: 6,070,244, hereinafter "Orchier").

Claims 11, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. and Orchier et al. as applied to claim 1, 12 respectively above, and further in view of Smid et al. (US Patent Number: 4,386,233, hereinafter "Smid").

These rejections are set forth in a prior Office Action, mailed on March 1st, 2005.

(11) Response to Argument

Issue #1:

Group #1: claims 1, 12, and 23-27.

Appellant argues on page 14 of the brief that the manner of execution of the modules is configured.

In response, it is still not clear what is configured, the module or the execution of the modules. Furthermore, it is not clear which device configures the modules or their execution, and how the two limitations are different. The "commands execute" and "are processed" refer to the same set of commands, but the first limitation ("the commands execute") appear to make the commands take a more active role in the execution, while the second limitation ("the commands are processed") appear to make something else, whatever extracts and executes the modules, be the active part of the execution.

Issue #2:

Group #1: claims 1, 6, 9-10, 12, 17, 20-21, 23-30, and 32.

Regarding claim 1, Appellant argues that

- **a)** Shostack teaches away from the claim language "wherein the commands execute the risk-assessment modules in a specific manner that is configured at the remote computer"; and
- **b)** Orchier fails to teach "wherein the commands are processed by extracting parameters associated with the commands and executing the risk-assessment modules indicated by the commands utilizing the associated parameters"

Regarding **a)**, Examiner points to column 2, lines 49-54 and column 4, lines 1-12 of Shostack, where the commands execute in a manner that is configured at the remote computer. The system of Shostack pushes updates to remote locations wherein the database of security vulnerabilities is updated, thus providing enhancements to the database and using that information to provide security solutions to potentially weak computer networks and/or computers (column 4, lines 1-12).

Regarding **b)**, Examiner points to Orchier's teachings: the query agent supports queries (commands with parameters) on the following data objects: user accounts, security groups, etc (column 13, lines 55-67) and the maintenance agent takes inputs from the user and converts them to platform independent instructions (column 14, lines 25-43). As clearly stated by Orchier in column 14, lines 28-43, the command AddUserAccount(id, platformList, name, PayrollNumber, expenseCode), the command

AddUserAccount takes the parameters id, platformList, name, PayrollNumber, expenseCode. Examiner also points to claim 28 (column 17, lines 53-63, column 18, lines 18) of the Orchier reference where "the commands are converted to a plurality of specific security commands configured to be understood by corresponding of ones of said security domains".

Assuming arguendo that Shostack and Orchier do not teach, separately or in combination, "wherein the commands are processed by extracting parameters associated with the commands and executing the risk-assessment modules indicated by the commands utilizing the associated parameters", Examiner submits that executing commands or modules, processing commands by extracting parameters associated with the commands was conventional and very well known, i.e. in a Unix system, a conventional user would execute a "cd ../" command to change directories, "mkdir temp" to create a directory (folder) named "temp", or an administrator user (root) could execute a command such as "passwd" and pass as a parameter to the "passwd" command a username account to change the password for the user associated with the specified username.

Computer commands in general take one or more parameters (sometimes called arguments), few commands exist that take none.

Group #2: claims 4 and 15.

Regarding claims 4 and 15, Appellant argues that Orchier fails to teach "wherein the risk-assessment modules are selected for the agent based on specifications of the local computer".

In response, attention is directed to column 4, lines 48-62, and column 5, lines 1-30 of the Orchier reference. Orchier expressly teach selecting modules (agents) based on specifications of the local computer (column 4, lines 48-62, column 5, lines 1-30, column 8, lines 47-64). Furthermore, Orchier's modules are specific to different platforms. The different modules (agents) of Orchier are based on the platform associated with the local computers, otherwise the agents would not be able to perform, i.e. an agent associated with operating system A (a platform), not only may not work on operating system B (another platform), but may attempt to collect vulnerabilities that do not apply to operating system B.

Group #3: claims 5 and 16.

Regarding claims 5 and 16, Appellant argues on pages 13-14 that Shostack fails to teach "wherein the risk-assessment modules include a STAT module for performing a stat system call on a file, a READ module for reading a file, a READDIR module for returning contents of a directory, a FIND module for locating a list of files based on a given function, a GETPWENT module for retrieving an entry from a password database, a GETGRENT module for retrieving an entry from a group database, a CHKSUM

module for performing a checksum operation on a file, and an EXEC module for executing a command.

In response, attention is directed to the different functionality each module in Shostack provides, the fact that Appellant calls the modules as STAT, READ, READDIR, FIND, GETPWENT, GETGRENT, CHKSUM, and EXEC modules is irrelevant to the fact that the functionality provided by Shostack's modules and Appellant's modules is similar, namely to detect security vulnerabilities on computers and networks.

Group #4: claim 34.

Regarding claim 34, Appellant argues on pages 14-15 that Shostack teaches a first module, not multiple risk assessment modules and that it simply discloses a first module that checks an operating system.

In response, Examiner points to the first two lines cited by Appellant, where Shostack clearly discloses **various integrated security system modules** (emphasis added) and furthermore to the remaining of column 12, where each module is described. The modules provide functionality to check for vulnerabilities on the operating system, the network, user passwords, etc, with a plurality of commands associated with each module. Shostack teaches six modules, all with different functionality. The **first module** checks for operating system vulnerabilities, the **second module** accesses the database of security vulnerabilities and assesses network security, the **third module** accesses the database of security vulnerabilities and

assesses security vulnerabilities in the passwords being used to access a computer or a computer network, etc.

Group #5: claim 31.

Regarding claim 31, Appellant argues on pages 15-16 that Shostack fails to teach "wherein the feedback includes descriptions as to how to correct the vulnerabilities".

Examiner points to column 4, lines 8-12 where the database of security vulnerabilities is described. Furthermore, Examiner stated on the Final Office Action that having a database of vulnerabilities and the means to generate report logs of the vulnerabilities found, it would have been obvious to one of ordinary skill in the art to at the time the invention was made to generate a log including how to correct the vulnerabilities. Further, on column 13, lines 36-44, Shostack teaches providing a reporting mechanism for reporting various network transactions. Shostack also teaches creating a report of the vulnerability (column 9, lines 58-63). Assuming arguendo that Appellant is correct and Shostack does not teach the claimed subject matter, Examiner submits that having the database of vulnerabilities as disclose by Shostack, with the columns as disclosed on Table 1, namely "Feature" and "Vulnerability" columns, it would have been obvious to add an additional column (Shostack, column 14, lines 29-34) to provide some additional information.

Group #6: claim 35.

Appellant argues on pages 16-17 of the brief that Orchier fails to teach "wherein a different set of risk-assessment modules exist on different local computers, based on a platform associated with each of the local computers".

In response, attention is directed to Orchier's teaching of a plurality of collection agents specific to particular platforms (column 4, lines 48-62, column 8, lines 47-64). The different modules (agents) of Orchier are based on the platform associated with the local computers, otherwise the agents would not be able to perform, i.e. an agent associated with operating system A (a platform), not only may not work on operating system B (another platform), but may attempt to collect vulnerabilities that do not apply to operating system B.

Issue #3:

Group #1: claims 11 and 22.

Appellant argues on pages 17-18 of the brief that Smid fails to teach decrypting commands using a shared key.

In response, attention is directed to column 2, lines 57-67, where Smid teaches using a key which is accessible only to authorized users and authenticating a user of a cryptographic function as a condition to access an interchange key. Furthermore, on column 6, lines 35-45, Smid teaches an interchange key which is used to connect all users, thus sharing the key.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

David Garcia Cervetti
September 6, 2005

Conferees
Christopher Revak
Ayaz Sheikh

9/5/05

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120